

ZTA-browsergebaseerde storing van TLS-handdruk voor privébronnen

Inhoud

uitgifte

Gebruikers hebben geen toegang tot een browsergebaseerde privébron via Cisco Secure Access.

Wanneer u probeert verbinding te maken, treden deze symptomen op:

- TCP drieweg handdruk voltooid met succes, maar TLS-onderhandeling mislukt na de Client Hello.
- De verbinding met de openbare SSE-toegewezen URL (<https://example-orgid.ztna.sse.cisco.io>) bereikt de Cisco-verificatie, maar geeft de HTTP 404-fout terug.
- Nadat de FQDN is toegevoegd aan de configuratie van de privébron, wordt het verkeer doorgestuurd naar de verificatieprompt, maar na de verificatie wordt een lege pagina weergegeven.
- HAR-bestanden tonen HTTP 200-reacties, maar TLS-handshake is niet voltooid.
- Blokreden wordt weergegeven als: "Privé-toegang: opgehaalde posturatiegegevens voor apparaat zijn te oud / moeten worden vernieuwd".

milieu

- Cisco Secure Access (SSE)
- ID Secure Access-organisatie: xxxx
- Zero Trust Network Access (ZTNA) op browserbasis
- Particuliere bron: example.net

- Werkende privébron voor vergelijking: abc.net
- Configuratie wildcard-certificaat

resolutie

Het probleem is opgelost door de private resource zodanig te configureren dat dezelfde certificaatconfiguratie wordt gebruikt als een werkende private resource.

De stappen die in de volgende secties worden beschreven, zijn genomen.

Stap 1: Werkende configuratie analyseren

Vergelijk de falende private resource (example.net) met een werkende private resource (abc.net) om configuratieverschillen te identificeren.

De gebruikte werkbron:

- Gebruik een URL in je domein optie
- Verwijzing naar het bestaande jokercertificaat/sleutelpaar

Stap 2: Analyse van pakketvastlegging

Analyse van pakketvastlegging uitvoeren met Wireshark om de TLS-handdruk te bevestigen:

- Verifieer of de TCP-handdruk in drie richtingen is voltooid.
- Bevestig dat TLS-onderhandelingen mislukken nadat Client Hello is geactiveerd.
- Verzamel diagnostische artefacten: HAR-bestanden, DART-bundel en pakketopnames.

Stap 3: Certificaatverificatie

Toegang tot de applicatie via RAVPN-verbinding om de certificaatpresentatie te verifiëren:

- Bevestig dat de website example.net een wildcard-certificaat presenteert.
- Documentcertificaatgegevens voor configuratiereferentie.

Stap 4: Privébron configureren

Pas dezelfde configuratiebenadering toe die wordt gebruikt door de werkende privébron:

- Configureer de privébron om een URL in uw domein te gebruiken optie.
- Verwijs naar het bestaande jokercertificaat/sleutelpaar.
- Controleer of het FQDN correct is geconfigureerd in het veld Privébron.

Stap 5: Validatie

Test browsergebaseerde toegang om te bevestigen dat de configuratie het probleem oplost:

- Controleren of de TLS-handdruk succesvol is voltooid.
- De juiste verificatiestroom bevestigen.
- Toegankelijkheid van toepassingen na verificatie valideren.

Oorzaak

De hoofdoorzaak was een configuratie-mismatch in de configuratie van de privébron. De defecte privébron is niet geconfigureerd om het jokercertificaat dat de doeltoepassing weergeeft, correct te kunnen raadplegen. De TLS-handshake is mislukt omdat de configuratie van de privébron niet is afgestemd op de certificaatconfiguratie die door de toepassingsserver wordt gebruikt. Door de privébron te configureren om de optie Een URL gebruiken in uw domein te gebruiken en te verwijzen naar het bestaande jokercertificaat/sleutelpaar (dat overeenkomt met de werkconfiguratie), kan de TLS-onderhandeling met succes worden voltooid.

Gerelateerde inhoud

- [Cisco Reference Guide voor beveiligde toegang](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.